



**eSecurity Advisory**  
**DECEMBER 2006 MICROSOFT SECURITY BULLETIN RELEASE**

This alert is to provide you with an overview of Security Bulletins released on 12 December 2006.

**NEW BULLETINS**

Microsoft is releasing the following security bulletins for newly discovered vulnerabilities:

MAXIMUM SEVERITY	BULLETIN NUMBER	PRODUCTS AFFECTED	IMPACT
<b>Critical</b>	MS06-072	Microsoft Windows	Remote Code Execution
<b>Critical</b>	MS06-073	Microsoft Visual Studio 2005	Remote Code Execution
<b>Important</b>	MS06-074	Microsoft Windows	Remote Code Execution
<b>Important</b>	MS06-075	Microsoft Windows	Elevation of Privilege
<b>Important</b>	MS06-076	Microsoft Outlook Express	Remote Code Execution
<b>Important</b>	MS06-077	Microsoft Windows	Remote Code Execution
<b>Critical</b>	MS06-078	Microsoft Windows Media Formats	Remote Code Execution

Summaries for these new bulletins may be found at the following page:  
<http://www.microsoft.com/technet/security/bulletin/ms06-Dec.aspx>

Re-released Bulletins

In addition, Microsoft is re-releasing the following security bulletin:

MAXIMUM SEVERITY	BULLETIN NUMBER	PRODUCTS AFFECTED (re-release only)	IMPACT
<b>Critical</b>	MS06-059	Microsoft Excel	Remote Code Execution

Information on this re-released bulletin may be found at the following page:

MS06-059 (Excel) – <http://www.microsoft.com/technet/security/bulletin/MS06-059.aspx>

**Agencies are advised to review the information in the bulletins, test and deploy the updates immediately in their environments, if applicable.**

Microsoft Windows Malicious Software Removal Tool

Microsoft is releasing an updated version of the Microsoft Windows Malicious Software Removal Tool on Windows Server Update Services (WSUS), Windows Update (WU) and the Download Center. Note that this tool will NOT be distributed using Software Update Services (SUS). Information on the Microsoft Windows Malicious Software Removal Tool can be located here:

<http://go.microsoft.com/fwlink/?LinkId=40573>

## eSecurity Advisory: DECEMBER 2006 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information

December 14, 2006

High-Priority Non-Security Updates on Microsoft Update (MU), Windows Update (WU), Windows Server Update Services (WSUS) and Software Update Services (SUS)

Microsoft is today also making the following High-Priority **NON-SECURITY** updates available on WU, MU, SUS and WSUS:

KB NUMBER	TITLE	Available via:
911897	Update for Windows Server	WU, MU
926251	Update for Windows XP Media Center Edition for 2005	WU, MU
928388	Update for Windows	WU, MU
929120	Update for Windows	WU, MU
924886	Update for Office 2003	MU

Listed below is more technical information that may be helpful to users to protect their work and home computers.

---

### MS06-072

**Title:** Cumulative Security Update for Internet Explorer (925454)

**Affected Software:**

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition

**Non-Affected Software:**

- Windows Vista

**Affected Components:**

- Microsoft Internet Explorer 5.01 Service Pack 4 on Windows 2000 Service Pack 4
- Microsoft Internet Explorer 6 Service Pack 1 when installed on Windows 2000 Service Pack 4
- Microsoft Internet Explorer 6 for Windows XP Service Pack 2
- Microsoft Internet Explorer 6 for Windows XP Professional x64 Edition
- Microsoft Internet Explorer 6 for Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Internet Explorer 6 for Windows Server 2003 for Itanium-based Systems and Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Internet Explorer 6 for Windows Server 2003 x64 Edition

**Non-Affected Components:**

- Windows Internet Explorer 7 for Windows XP Service Pack 2

## eSecurity Advisory: DECEMBER 2006 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information  
December 14, 2006

- Windows Internet Explorer 7 for Windows XP Professional x64 Edition
- Windows Internet Explorer 7 for Windows Server 2003 Service Pack 1
- Windows Internet Explorer 7 for Windows Server 2003 with SP1 for Itanium-based Systems
- Windows Internet Explorer 7 for Windows Server 2003 x64 Edition
- Windows Internet Explorer 7 in Windows Vista

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Critical**

**Security Update Replacement:** This bulletin replaces several prior security updates. See the frequently asked questions (FAQ) section of this bulletin for the complete list.

**Caveats:** Microsoft Knowledge Base Article 925454 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 925454.

**Restart required:** You must restart your system after you apply this security update.

**Removal Information:** To remove this security update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-072.msp>

---

### MS06-073

**Title:** Vulnerability in Visual Studio 2005 Could Allow Remote Code Execution (925674)

**Affected Software:**

- Microsoft Visual Studio 2005
  - Visual Studio 2005 Standard Edition
  - Visual Studio 2005 Professional Edition
  - Visual Studio 2005 Team Suite
  - Visual Studio 2005 Team Edition for Developers
  - Visual Studio 2005 Team Edition for Architects
  - Visual Studio 2005 Team Edition for Testers

**Non-Affected Software:**

- Microsoft Visual Studio 2005
  - Visual Basic 2005 Express Edition
  - Visual C++ 2005 Express Edition
  - Visual C# Express Edition
  - Visual J# Express Edition

## eSecurity Advisory: DECEMBER 2006 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information

December 14, 2006

- Visual Web Developer Express Edition
- Visual Studio 2005 Tools For Office
- Visual Studio 2005 Team Explorer
- Visual Studio 2005 Team Foundation Dual-Server
- Visual Studio 2005 Team Foundation Single Server
- Visual Studio 2005 Team Foundation Proxy
- Visual Studio 2005 Team Foundation Build
- Visual Studio 2005 Premier Partner Edition
- Microsoft Visual Studio 6.0 Service Pack 6
- Microsoft Visual Studio .NET 2002 Service Pack 1
- Microsoft Visual Studio .NET 2003 Service Pack 1

**Note:** Not all versions of Visual Studio 2005 include the affected file. If you do not have wmscriptutils.dll on your system you are not affected by this vulnerability

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Critical**

**Security Update Replacement:** None

**Caveats:** Microsoft Knowledge Base Article 925674 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 925674.

**Restart required:** In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.

**Removal Information:** To remove this security update, use the Add or Remove Programs tool in Control Panel.

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-073.msp>

---

### MS06-074

**Title:** Vulnerability in SNMP Could Allow Remote Code Execution (926247)

**Affected Software:**

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

- Microsoft Windows Server 2003 x64 Edition

**Non-Affected Software:**

- Windows Vista

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Important**

**Security Update Replacement:** None

**Caveats:** None

**Restart required:** This update requires a restart.

**Removal Information:** To remove this security update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-074.msp>

---

**MS06-075**

**Title:** Vulnerability in Windows Could Allow Elevation of Privilege (926255)

**Affected Software:**

- Microsoft Windows XP Service Pack 2
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 for Itanium-based Systems

**Non-Affected Software:**

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 with Service Pack 1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition
- Windows Vista

**Impact of Vulnerability:** Elevation of Privilege

**Maximum Severity Rating:** **Important**

**Security Update Replacement:** None

**Caveats:** None

**Restart required:** This update requires a restart.

**Removal Information:** To remove this security update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-075.msp>

---

## **MS06-076**

**Title:** Cumulative Security Update for Outlook Express (923694)

### **Affected Software:**

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition

### **Non-Affected Software:**

- Windows Vista

### **Affected Components:**

- Outlook Express 5.5 Service Pack 2 on Microsoft Windows 2000 Service Pack 4
- Outlook Express 6 Service Pack 1 when installed on Microsoft Windows 2000 Service Pack 4
- Outlook Express 6 on Microsoft Windows XP Service Pack 2
- Outlook Express 6 on Microsoft Windows XP Professional x64 Edition
- Outlook Express 6 on Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Outlook Express 6 on Microsoft Windows Server 2003 x64 Edition
- Outlook Express 6 on Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Important**

**Security Update Replacement:** This bulletin replaces several prior security updates. See the frequently asked questions (FAQ) section of the bulletin for the complete list.

## eSecurity Advisory: DECEMBER 2006 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information

December 14, 2006

**Caveats:** Microsoft Knowledge Base Article 923694 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 923694.

**Restart required:** This update does not require a restart. The installer stops the required services, applies the update, and then restarts the services. However, if the required services cannot be stopped for any reason, or if required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.

**Removal Information:** To remove this security update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-076.mspx>

---

### MS06-077

**Title:** Vulnerability in Remote Installation Service Could Allow Remote Code Execution (926121)

**Affected Software:**

- Microsoft Windows 2000 Service Pack 4

**Non-Affected Software:**

- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition
- Windows Vista

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Important**

**Security Update Replacement:** None

**Caveats:** Microsoft Knowledge Base Article 926121 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 926121.

**Restart required:** This update requires a restart.

**Removal Information:** To remove this security update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-077.msp>

---

## **MS06-078**

**Title:** Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689)

### **Affected Software:**

- Microsoft Windows Media Format 7.1 through 9.5 Series Runtime on the following operating system versions:
  - Microsoft Windows 2000 Service Pack 4
  - Microsoft Windows XP Service Pack 2
  - Microsoft Windows XP Professional x64 Edition
  - Microsoft Windows Server 2003 or Microsoft Windows Server 2003 Service Pack 1
  - Microsoft Windows Server 2003 x64 Edition
- Microsoft Windows Media Format 9.5 Series Runtime x64 Edition on the following operating system versions:
  - Microsoft Windows XP Professional x64 Edition
  - Microsoft Windows Server 2003 x64 Edition
- Microsoft Windows Media Player 6.4
  - Windows 2000 Service Pack 4
  - Microsoft Windows XP Service Pack 2
  - Microsoft Windows XP Professional x64 Edition
  - Microsoft Windows Server 2003 or on Microsoft Windows Server 2003 Service Pack 1
  - Microsoft Windows Server 2003 x64 Edition

### **Non-Affected Software:**

- Windows Vista
- Microsoft Windows 2003 For Itanium-Based Systems and Windows Server 2003 with SP1 for Itanium-based Systems
- Windows Media Format 11 Series when installed on all Microsoft Operating Systems

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Critical**

**Security Update Replacement:** None

**Caveats:** None

**Restart required:** This update does not require a restart. The installer stops the required services, applies the update, and then restarts the services. However, if the required services cannot be stopped

## eSecurity Advisory: DECEMBER 2006 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information  
December 14, 2006

for any reason, or if required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.

**Removal Information:** To remove this update, use the Add or Remove Programs tool in Control Panel. Note Before upgrading your Windows Media Format Series Runtime, we recommend you uninstall this update and re-install after you have finished upgrading.

System administrators can also use the Spuninst.exe utility to remove this security update.

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-078.mspx>

---

### **MS06-059 (Re-released)**

**Title:** Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (924164)

**Affected Software:** Please see the security bulletin for details on affected software.

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Critical**

**Reason for Re-release:** Bulletin updated has been revised and re-released for Microsoft Excel 2002 to address the issues identified in Microsoft Knowledge Base Article 924164.

**More information on this re-released bulletin is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-059.mspx>